FAQ: Security

SECURITY: Frequently Asked Questions

Comentado [CR1]: @Mike Sparling last one I promise!! Since there are ony two questions I will absorb this onfo into one of the other docs where it makes most sense.

MHS values, respects and protects all personal data of its customers, the data of their clients, and data collected through electronic commerce practices, with the highest level of security. MHS limits the use of this information to the purposes outlined on our consent agreements and holds such information within the strictest confidence. This applies to both online and offline information that is collected and used in the course of providing you with our products and services. MHS adheres to various regulations such as PIPEDA, FERPA, HIPAA, and GDPR.

How does MHS protect Personal Information and ensure Data Security?

Personal information, understood to be any information that identifies or could be used to identify an individual. Personal Information is protected by MHS through a number of safety measures encompassing all systems and interactions where personal information is collected and stored. MHS actively monitors all secure information reserves (including but not limited to Order Management Systems (OMS), digital data, ecommerce platforms, and hard copy records) to ensure security measures are maintained at the highest level of security, meeting all regulatory and legal requirements.

MHS servers use 128/256-bit industry-standard Secure Sockets Layer (SSL) encryption which is encryption technology that works with the most current web browsers. SSL encrypts the purchaser's personal information, including Financial Data and other personal data as well as test user information, including test data, responses, and reports returned to the Administrator, protecting against disclosure to third parties.

How is assessment data secured?

Access to data collected through online services including but not limited to scoring of assessments, is restricted to qualified users and requires an ID and password. Registration of MHS customers or their designated administrators ("Administrators") is rigorous with defined qualification user levels. Identity is confirmed by an Attestation of Qualification process which is a binding test user agreement coupled with a review of qualifications and/or certification.

After you have completed registration, MHS will, as a matter of policy keep on file a record of (i) the products and services you have purchased; (ii) your certification status; (iii) your contact information; and (iv) any aggregate de-personalized information including test data, indefinitely unless otherwise stipulated. Please note, once de-personalized any test results or related data will no longer be considered personal information and will remain an anonymous record with no baring or impact on the individual. In this state it will no longer be considered a record associated with any one individual and will not be subject to regulations related to personal information and the rights of an individual.

Comentado [CR2]: This is not the case with data saved in Rackspace as confirmed with Paul/Nick. We can reposition focusing on the security of protecting data which is in supportof Digital Trust.

Comentado [CR3]: Confirm this is at RackSpace or by MHS?

Comentado [CR4]: Although this statement is true in premise - if we don't store "depersonalized" data in Rackspace will delete.

What about an unauthorized access?

In the event that MHS becomes aware of a security breach which MHS believes has resulted in, or may result in a risk of harm in the unauthorized access, use or disclosure to non-public personnel information of our clients, MHS will promptly investigate the matter and notify the applicable parties of such breach. Detected through an Intrusion Detection System, an alert will be automatically triggered to MHS. An investigation will begin without delay, consistent with (1)

FAQ: Security

legitimate needs of law enforcement and the Privacy Commissioner’s Office; (2) measures necessary to determine the scope of the breach; (3) efforts to identify the individuals affected; and (4) steps to identify cause of breach and restore the reasonable integrity of our secure server.

For further information please contact the MHS Privacy Officer.

MHS Privacy Officer
Email: privacyofficer@mhs.com